Cấu trúc tựa đẳng cấu giữa vành đa thức có 2 lớp kề cyclic và trường số

On a Quasi-Isomorphic Structure Between Polynomial Ring with Two Cyclotomic Cosets and Finite Field

Lê Danh Cường*, Nguyễn Bình

Học viện Công nghệ Bưu chính Viễn thông, 122 Hoàng Quốc Việt , Cầu Giấy, Hà Nội

Tóm tắt

Bài toán Logarit rời rạc trong trường GF(p) là đối tượng trong nhiều công trình nghiên cứu và người ta có thể chọn giá trị p để Bài toán được xem là khó. Vành đa thức có 2 lớp kề cyclic $Z_2[x]/(x^n+1)$ là một loại vành đặc biệt chỉ có 2 lũy đẳng. Bài báo đưa ra cấu trúc tựa đẳng cấu giữa vành đa thức có 2 lớp kề cyclic và trường $GF(p)$ với $p=2^n-1$ là một số nguyên tố Mersenne chỉ có 1 lũy đẳng. Các kết luận về sự tựa đẳng cấu này là kết quả của các phân tích toán học và được minh họa bằng các ví dụ cụ thể. Dựa trên quan hệ tựa đẳng này, ta có thể dễ dàng xây dựng được bài toán logarithm rời rạc trên các vành đa thức. Từ đó cho phép ứng dụng trong giải quyết các vấn đề mật mã (xác thực, chữ ký số, mã hóa.v.v.) đối với các hệ mật

Từ khóa: Vành đa thức với 2 lớp kề cyclic, bài toán logarithm rời rạc, phần tử sinh, đa thức bất khả quy, tựa đẳng cấu.

Abstract

The well-known problem of computing discrete logarithms in finite field GF(p) has acquired importance in many studies due to its applicability in cryptography. This is widely thought to be very computationnaly hard if large prime p is selected. Polynomial ring with two cyclotomic cosets $Z_2[x]/(x^n+1)$ is a special ring with only two idempotent elements. In this paper, a quasi-isomorphic structure between polynomial ring with two cyclotomic cosets $Z_2[x]/(x^n+1)$ and field $GF(p)$ with only one idempotent element (where $p=2^n-1$ is Mersenne primer) is presented. Conclusions on this isomorphism are the result of mathematical analysis and are illustrated by concrete examples. Based on this structure we can construct Discrete logarithm problem over polynomial rings. Discrete logarithm problem over polynomial rings can be used in many cryto-systems (for authentication, digital signatures, encryption.etc..).

Keywords: Polynomial ring with two cyclotomic cosets, Discrete logarithm problem, $GF(p)$ Field, primitive element, irreducible polynomial, quasi-isomorphic structure.

1. Giới thiệu

1.1. Vành đa thức có 2 lớp kề cyclic

Định nghĩa 1: Vành đa thức theo modulo x^n+1 được gọi là vành đa thức có hai lớp kề cyclic nếu phân tích của x^n+1 dưới dạng tích các đa thức bất khả quy trên trường $GF(2)$ có dạng:

$$x^n+1=(x+1)\sum_{i=0}^{n-1}x^i \qquad (1)$$

trong đó $(x+1)$ và $\sum_{i=0}^{n-1}x^i$ là các đa thức bất khả quy [1, 2]

Ví dụ: $n=5,11,19,29,31,..$

$$x^5+1=(x+1)(x^4+x^3+x^2+x+1)$$

Bổ đề 1: Vành đa thức với 2 lớp kề cyclic có thể được phân hoạch như sau:

A
$\overline{A}$
$e_0(x)$

* Địa chỉ liên hệ: Tel.: (+84) 923.207.666
Email: cuongqt34@yahoo.com

trong đó A và $\overline{A}$ là các nhóm nhân cyclic có cấp cực đại max $ord[a(x)] = 2^{n-1} - 1$ với phần tử sinh $a(x)$ là đa thức trên vành $Z_2[x]/(x^n + 1)$

$$A = \{a^i(x), i = 1,2,..,2^{n-1} - 1\}$$

$$\overline{A} = \{\overline{a}^i(x), i = 1,2,..,2^{n-1} - 1\}$$

trong đó cấp của $a(x)$ sẽ là k

Định nghĩa 2: Cho $f(x) \in Z_2[x]/(x^n + 1)$, khi đó $e_0(x) = \sum_{i=1}^{n-1} x^i$ được gọi là lũy đẳng nuốt.

Ta có: $e_0(x) = e_0^{\,2}(x) \bmod(x^n + 1)$

Hệ quả: Với $f(x) \in Z_2[x]/(x^n + 1)$ thì

$$f(x).e_n(x) = \begin{cases} e_n(x) & if\ W(f(x))\ le \\ 0 & if\ W(f(x))\ chan \end{cases}$$

$W(f(x))$ là trọng số của đa thức $f(x)$ (2)

Định nghĩa 3: Đa thức $\overline{a}(x)$ được gọi là đa thức đối xứng với đa thức $a(x)$ nếu

$$a(x) = \sum_{i \in I} a_i x^i \text{ thì } \overline{a}(x) = \sum_{j \in J} a_j x^j \qquad (3)$$

Trong đó $I \cap J = \emptyset$; $I \cup J = Z_n$

Dựa vào tính chất của lũy đẳng nuốt, ta có

$$\overline{a}(x) = e_0(x) + a(x) \qquad (4)$$

1.2. Trường số $GF(p)$

Ta quan tâm tới tính chất nguyên tố được phát biểu như sau:

$GF(p)$ là một trường khi và chỉ khi p là số nguyên tố. Nhưng $p = 2^n - 1$ là số nguyên tố khi và chỉ khi n là số nguyên tố và thỏa mãn bổ đề sau đây [4]:

Cho trước số nguyên tố lẻ q. Ta xác định dãy số $\{L_n\}$ sau:

$L_0 = 4$, $L_{n+1} = (L_n^2 - 2) \bmod(2^q - 1)$, với $\forall n = 0,1,2,..$ Khi đó, $2^q - 1$ là số nguyên tố $\Leftrightarrow L_{q-2} \equiv 0 \bmod(2^q - 1)$

Xét $p = 2^n - 1$ là số nguyên tố.

Khi đó $Z_p \leftrightarrow GF(p)$, $Z_p^* = Z_p / \{0\}$ là một nhóm nhân cyclic cấp $|Z_p^*| = 2^n - 2$ với $a \in Z_p^* \rightarrow \exists b \in Z_p^*$: $a.b \equiv 1 \bmod p$

Xét $W(a(x))$ lẻ. Khi đó, $\exists b(x)$ với $W(b(x))$ lẻ thỏa mãn $a(x).b(x) \equiv 1 \bmod(x^n + 1)$

Ta xây dựng phép tương ứng sau:

$$a(x) = \sum_{i \in I} f_i x^i \rightarrow a = \sum_{i \in I} f_i 2^i \in Z_p^*$$

Xét trường hợp $e_0(x) = \sum_{i=0}^{n-1} x^i = 0$. Khi đó ta có thể coi đây là một ánh xạ 1-1 giữa các phần tử của $Z_2[x]/(x+1)$ và các phần tử của $GF(p)$

Ví dụ 1: Nhóm nhân cyclic trên Z_{31} với phần tử sinh (nguyên thủy) $a = 3$

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3^i	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
3^i	28	22	4	12	5	15	14	11	2	6	18	23	7	21	1

Số phần tử nguyên thủy trong nhóm Z_{31}^*

$N = \varphi(31-1) = \varphi(30) = 8$

Đó là các phần tử dạng 3^i, với $(i,30) = 1$, chúng thuộc tập $\{3,17,13,24,22,12,11,21\}$

Ví dụ 2: Các nhóm nhân cyclic trên $Z_2[2]/(x^5 + 1)$

$$A = \{(024), (034), (1), (013), (014), (2), (124), (012), (3)(023), (123), (4), (134), (234), (0)\}$$

$$\overline{A} = \{(13), (12), (0234), (24), (23), (0134), (03), (34), (0124), (14), (04), (0123), (02), (01), (1234)\}$$

Hay $A = \{21,25,2,11,19,4,22,7,8,13,14,16,26,28,1\}$
$\overline{A} = \{10,6,29,20,12,27,9,24,23,18,17,15,5,3,30\}$ Số phần tử nguyên thủy trong mỗi nhóm cyclic này cũng là 8

2. Mối quan hệ giữa $Z_2[x]/(x^n+1)$ và $GF(p)$

Định nghĩa 4: Với phép ánh xạ nêu trên, vành đa thức có hai lớp kề cyclic và trường số $GF(p)$ với $p = 2^n - 1$ nguyên tố được gọi là tựa đẳng cấu (quasi-isomorphism).

Ta có thể so sánh việc thực hiện các phép toán cộng và nhân trên hai cấu trúc này qua các ví dụ như sau:

Phép toán	Vành đa thức $Z_2[x]/(x^n+1)$	Trường số $GF(p)$
Phép cộng	$a(x) = \sum_{i\in I\subset Z_n} a_i x^i$ $b(x) = \sum_{j\in J\subset Z_n} b_j x^j$ $a(x)+b(x) = c(x)$ $c(x) = \sum_{k\in K\subset Z_n} c_k x^k$ $K = (I\cup J)\setminus(I\cap J)$	$a,b \in GF(p)$ $a + b \equiv (a + b) \mod p$
Phép nhân	$a(x).b(x) \equiv a(x).b(x) \mod(x^n+1)$	$a.b \equiv a.b \bmod p$

Ví dụ 3

Phép toán	Vành đa thức $Z_2[x]/(x^5+1)$	Trường số $GF(31)$
Phép cộng	$a(x) = 1+x+x^3$ $b(x) = 1+x^3+x^4$ $a(x)+b(x) = c(x)$ $c(x) = (x+x^4)$ $\mod(x^5+1) = x^2+1$	$a = 11$ $b = 25$ $a+b \equiv (11+25) \bmod 31 = 5$
Phép nhân	$a(x).b(x) \equiv a(x).b(x) \mod(x^5+1)$ $a(x).b(x) \equiv (1+x+x^3)(1+x^2+x^4) \bmod(x^5+1)$ $= x^4+x+1$ $a(x).b(x) \equiv (1+x+x^4)$	$a.b \equiv (11.21) \bmod 31 = 14$

Ví dụ 4: Các phần tử nghịch đảo

TT	Trên $Z_2[x]/(x^5+1)$: $a(x).b(x) \equiv 1 \bmod(x^n+1)$	Trường số $GF(31)$: $a.b \equiv 1 \bmod 31$
1	$a(x) = (234), b(x) = (024)$ $(x^4+x^3+x^2)(x^4+x^2+1) \equiv 1 \bmod(x^5+1)$	$3.21 \equiv 1$
2	$a(x) = (124), b(x) = (012)$ $(x^4+x^2+x)(x^2+x+1) \equiv 1 \bmod(x^5+1)$	$9.7 \equiv 1$
3	$a(x) = (2), b(x) = (3)$ $x^2.x^3 \equiv 1 \bmod(x^5+1)$	$27.23 \equiv 1$
4	$a(x) = (014), b(x) = (023)$ $(x^4+x+1)(x^3+x^2+1) \equiv 1 \bmod(x^5+1)$	$19.18 \equiv 1$
5	$a(x) = (134), b(x) = (034)$ $(x^4+x^3+x)(x^4+x^3+1) \equiv 1 \bmod(x^5+1)$	$26.6 \equiv 1$
6	$a(x) = (4), b(x) = (1)$ $x^4.x \equiv 1 \bmod(x^5+1)$	$16.2 \equiv 1$
7	$a(x) = (123), b(x) = (013)$ $(x^3+x^2+1)(x^3+x+1) \equiv 1 \bmod(x^5+1)$	$17.11 \equiv 1$
8	$a(x) = (013), b(x) = (123)$ $(x^3+x+1)(x^3+x^2+1) \equiv 1 \bmod(x^5+1)$	$20.14 \equiv 1$
9	$a(x) = (1), b(x) = (4)$ $x.x^4 \equiv 1 \bmod(x^5+1)$	$29.15 \equiv 1$
10	$a(x) = (034), b(x) = (134)$	$25.5 \equiv 1$

	$(x^4+x^3+1)(x^4+x^3+x)\equiv 1 \bmod(x^5+1)$	
11	$a(x)=(023), b(x)=(014)$ $(x^3+x^2+1)(x^4+x+1)\equiv 1 \bmod(x^5+1)$	$13.12\equiv 1$
12	$a(x)=(3), b(x)=(2)$ $x^3.x^2\equiv \bmod(x^5+1)$	$8.4\equiv 1$
13	$a(x)=(012), b(x)=(124)$ $(x^2+x+1)(x^4+x^2+1)\equiv 1 \bmod(x^5+1)$	$24.22\equiv 1$
14	$a(x)=(024), b(x)=(234)$ $(x^4+x^2+1)(x^4+x^3+x^2)\equiv 1 \bmod(x^5+1)$	$10.28\equiv 1$
15	$a(x)=(0), b(x)=(0)$	$30.30\equiv 1$

3. Kết luận

Vành đa thức có 2 lớp kề cyclic là một loại vành đặc biệt chỉ có 2 lũy đẳng, và vì vậy nó khá tương đồng với trường số $GF(p)$ chỉ có lũy đẳng 1. Ta có thể sử dụng quan hệ tựa đẳng cấu này để xây dựng bài toán logarithm rời rạc và hệ mật tựa ElGamal trên vành đa thức có 2 lớp kề cyclic [3].

Tài liệu tham khảo

[1] Menezes A. J., Van Oorchot P. C., "Handbook of Applied Cryptography", CRC Press, 1998;

[2] Đặng Hoài Bắc, "Các mã cyclic và cyclic cục bộ trên vành đa thức có hai lớp kề cyclic", Luận án Tiến sĩ Kỹ thuật, Học viện Công nghệ Bưu chính Viễn thông, 2010;

[3] Nguyễn Bình, "Hệ mật tựa ElGamal trên vành đa thức có 2 lớp kề cyclic", Tạp chí Khoa học và công nghệ , 2012

[4] Donald E.Knuth, ''The Art of computer programming'', 1968.